LES GUIDES DE LA CNIL



GUIDE « INFORMATIQUE ET LIBERTÉS »

POUR L'ENSEIGNEMENT DU SECOND DEGRÉ

Édition 2010





Sommaire

Ce guide est téléchargeable sur le site Internet de la CNIL : www.cnil.fr



Avant-propos

Un recours croissant à l'usage des technologies de l'information exige que chacun de nous respecte les principes du droit à la protection des données personnelles dans ses deux volets : droits individuels et obligations. C'est à ce prix que nos sociétés innoveront et se développeront dans le respect de la vie privée et des libertés des personnes. En la matière, le rôle du chef d'établissement, de son équipe et celui de la CNIL sont analogues pour faire en sorte que chaque citoyen, administré et futur citoyen maîtrise ces nouveaux outils et soit sensibilisé aux risques éventuels qu'ils peuvent représenter.

La loi « *Informatique et Libertés* » du 6 janvier 1978, modifiée par la loi du 6 août 2004, définit les principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles. Elle renforce les droits des personnes, prévoit une simplification des formalités déclaratives et précise les pouvoirs de contrôle et de sanction de la CNIL. Enfin, la création de la fonction de correspondant à la protection des données personnelles est l'occasion de diffuser la culture Informatique et Libertés.

C'est dans ce cadre que ce guide pratique a été rédigé afin d' apporter une réponse concrète à vos questions, que ce soit au sein de l'établissement (espace numérique de travail) ou à l'extérieur (sensibilisation des mineurs aux mesures à prendre pour éviter les risques d'atteinte à la vie privée).

Bien entendu, ce guide peut également soulever des questions, nous sommes à votre disposition pour y répondre.

Alex Türk

Président de la CNIL

PARTIE 1 : FICHES THÉMATIQUES

Fiche n°1 : Définitions des notions-clés de la loi « *Informatique et Libertés* »

La loi « *Informatique et Libertés* » est applicable dès lors qu'il existe un traitement automatisé ou un fichier manuel, c'est-à-dire un fichier informatique ou un fichier « *papier* » contenant des informations personnelles relatives à des personnes physiques.

A noter : Ne sont pas soumis à la loi les « *traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles* » tels que par exemple les agendas électroniques, les répertoires d'adresses, les sites internet familiaux en accès restreint.

Traitement de données à caractère personnel

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Exemples : Fichiers de gestion des étudiants et des personnels, annuaires en ligne des anciens diplômés, espaces numériques de travail.

Donnée à caractère personnel

Des données sont considérées comme à caractère personnel dès lors qu'elles permettent d'identifier directement ou indirectement des personnes physiques (ex. : nom, n° d'immatriculation, n° de téléphone, photographie, éléments biométriques tels que l'empreinte digitale, ADN, informations permettant de discriminer une personne au sein d'une population telles que, par exemple, le lieu de résidence, la profession, le sexe, l'âge, etc.).

Il peut en effet s'agir d'informations qui ne sont pas associées au nom d'une personne mais qui peuvent permettre de l'identifier et de connaître ses habitudes ou ses goûts.

Exemples : « *Le propriétaire du véhicule 3636AB75 est abonné à telle revue* » ou encore « *l'assuré social 1600530189196 va chez le médecin plus d'une fois par mois* ».

A noter : La loi « *Informatique et Libertés* » ne s'applique pas aux personnes morales (ex. : fichier de noms de sociétés, sauf s'il contient des noms de personnes physiques comme le nom du responsable commercial).

Responsable du traitement

- Est considéré comme le responsable du traitement la personne physique ou morale qui détermine les finalités et les moyens de toute opération (collecte, enregistrement, modification...), appliquée à des données à caractère personnel.

Le responsable du traitement est la personne pour le compte de laquelle est réalisé le traitement. Afin de déterminer l'identité du responsable du traitement, il est possible de faire appel aux critères suivants :

- celui de la « *maîtrise d'ouvrage* » du traitement : à quoi servira-t-il et comment fonctionnera-t-il ?

- celui de la « *mise en œuvre* » du traitement : qui décide de s'en servir et qui s'en sert ?

Exemple : En application de l'article R. 421-8 du code de l'éducation, le chef d'établissement est le représentant de l'État et l'organe exécutif de l'établissement public local d'enseignement (E.P.L.E) ; à ce titre, il détient la responsabilité de décider la création d'un traitement de données à caractère personnel et de procéder aux formalités liées à sa déclaration auprès de la CNIL.

En pratique : Le responsable du traitement sera notamment la personne en charge :

- de veiller au respect des principes de la protection des données personnelles ;

- d'informer les personnes au sujet de l'existence de leurs droits d'accès, de rectification et d'opposition ;

- de désigner, le cas échéant, un Correspondant Informatique et Libertés ;

- de procéder à l'accomplissement des formalités auprès de la CNIL, sauf en cas de désignation d'un Correspondant Informatique et Libertés[1].

- Le responsable du traitement doit être distingué des personnes qui interviennent dans le cadre de sa mise en œuvre telles que, par exemple, les sous-traitants. Le sous-traitant est un exécutant extérieur qui ne peut agir que sous l'autorité du responsable du traitement et sur instruction de celui-ci. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la loi. La sous-traitance ne décharge pas le responsable du traitement de sa responsabilité[2].

Exemple : Dans le cas d'un hébergement externe de l'un des sites web de l'établissement scolaire, l'hébergeur est considéré comme le sous-traitant.

1 Dans le cas de demande d'avis ou de demande d'autorisation, les formalités déclaratives auprès de la CNIL subsistent.
2 Se reporter à l'annexe 3 : modèle de clause de confidentialité dans le cadre d'un marché ou d'un contrat de sous-traitance.

Comment déclarer les transferts de données ?

Lorsque le transfert de données concerne un pays de l'Union européenne, il n'a pas à être autorisé par la CNIL.

En cas de transfert de données en dehors de l'Union européenne, le responsable de traitement (ex : hébergeur du site internet), doit le préciser sur le formulaire de déclaration et remplir une annexe « *transfert* ». Il doit aussi préciser les garanties de protection des données : existence de clauses contractuelles types issues des directives européennes, ou de règles internes d'entreprise (BCR), adhésion au *safe harbor* du destinataire des données.

Le transfert doit ensuite faire l'objet d'une autorisation par la CNIL, sauf dans certains cas bien spécifiques (par exemple : entreprise destinataire adhérente au *safe harbor*).

Pour toute information complémentaire sur ces questions, consulter le dossier « *International* » ou le « *Guide sur les transferts de données à caractère personnel vers des pays non-membres de l'Union européenne* » sur le site internet de la CNIL.

Fiche n°2 : Principes de la protection des données personnelles

Les informations que les établissements de l'enseignement secondaire traitent informatiquement pour remplir leurs missions de service public doivent être protégées parce qu'elles relèvent de la vie privée et parce que leur divulgation est susceptible de porter atteinte aux droits et libertés des personnes concernées.

La loi « *Informatique et Libertés* » a défini les principes à respecter lors de la collecte, du traitement et de la conservation de ces données. La loi prévoit également un certain nombre de droits pour les personnes dont les données personnelles ont été recueillies.

Le respect, par les établissements de l'enseignement secondaire des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard des personnes (étudiants, personnels). C'est aussi un gage de sécurité juridique pour les directeurs d'établissement qui, responsables des fichiers mis en œuvre, doivent veiller à ce que la finalité de chaque traitement informatique et les éventuelles transmissions d'informations soient clairement définies, les dispositifs de sécurité informatique précisément déterminés et les mesures d'information des usagers appliquées.

1. Le principe de finalité : une utilisation encadrée des fichiers

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions de l'établissement, responsable du traitement. C'est au directeur d'établissement qu'il appartient de fixer la finalité des traitements mis en œuvre pour le compte de son établissement et de la faire respecter.

A noter : Tout détournement de finalité est passible de sanctions pénales.

Exemple : Le fichier de gestion administrative et pédagogique des élèves ne peut être utilisé à des fins commerciales ou politiques.

2. Le principe de proportionnalité

Seules doivent être enregistrées les informations pertinentes et nécessaires pour assurer la gestion des services de l'établissement scolaire.

Exemple : Demander le revenu des parents de l'élève pour recevoir la « *newsletter* » de l'établissement n'est ni pertinent ni nécessaire au regard de la finalité poursuivie par le traitement.

3. Le principe de durée limitée de conservation des données : *« le droit à l'oubli »*

Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier.

Exemple : Les informations collectées dans le cadre de l'organisation d'un examen sont conservées pour la durée de la session de l'examen.

Au-delà, les données peuvent être archivées, sur un support distinct [3].

4. Le principe de sécurité et de confidentialité

Le directeur d'établissement, en tant que responsable du traitement, est astreint à une obligation de sécurité : il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation.

- Les données contenues dans les fichiers ne peuvent être consultées que par les services habilités à y accéder en raison de leurs fonctions.

Exemple : Veiller à ce que chaque utilisateur ait un mot de passe individuel régulièrement changé et que les modalités d'accès soient précisément définies en fonction des besoins réels.

- Le responsable du traitement doit prendre toutes les mesures pour empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Exemple : S'il est fait appel à un prestataire externe, des garanties contractuelles doivent être envisagées [4] .

- Les mesures de sécurité, tant physiques que logiques, doivent être prises.

Exemple : Protection anti-incendie, copies de sauvegarde, installation de logiciel antivirus, changement fréquent des mots de passe alphanumériques d'un minimum de 8 caractères.

- Les mesures de sécurité doivent être adaptées à la nature des données et aux risques présentés par le traitement.

Exemple : Authentification forte pour l'accès aux résultats d'examen, chiffrement des coordonnées bancaires transitant sur internet.

3 La durée de conservation déclarée dans le dossier de formalité adressé à la CNIL ou dans le registre du CIL doit correspondre à la période durant laquelle les données restent accessibles ou consultables directement par le personnel, par opposition avec la période d'archivage des données pendant laquelle celles-ci ne sont plus destinées à être utilisées à des fins de gestion et sont de ce fait, conservées sur un support distinct au sein d'un service d'archives. Se reporter à l'instruction ministérielle sur l'archivage (référence : DAF DPACI/RES/2005/003 du 22 février 2005).

4 Voir annexe 3 : modèle de clause de confidentialité dans le cadre d'un marché ou d'un contrat de sous-traitance.



5. Le principe du respect du droit des personnes

a) Informer les intéressés

Lors de l'informatisation de tel ou tel service, ou lorsque des données sont recueillies par exemple par voie de questionnaire, les usagers concernés et le personnel de l'organisme doivent être informés de la finalité du traitement, du caractère obligatoire ou facultatif du recueil, des destinataires des données et des modalités d'exercice des droits qui leur sont ouverts au titre de la loi « *Informatique et Libertés* » : droit d'accès et de rectification mais aussi, droit de s'opposer, sous certaines conditions, à l'utilisation de leurs données.

Cette information doit être diffusée, par exemple, au moyen d'affiches apposées dans les services recevant du public et portée sur les formulaires établis par l'établissement, ainsi que sur les courriers adressés aux personnes dont les données sont collectées.

En pratique : Des modèles de mentions d'information sont disponibles en annexe 3.

b) Les droits d'accès et de rectification

Toute personne (élève, enseignant, personnel) peut demander communication de toutes les informations la concernant contenues dans un fichier détenu par l'établissement et a le droit de faire rectifier ou supprimer les informations erronées.

c) Le droit d'opposition

Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que des données la concernant soient enregistrées dans un fichier informatique, sauf si celui-ci présente un caractère obligatoire.

Exemple : Le fichier de gestion administrative des élèves ou encore le fichier de gestion de prêts de livres de la bibliothèque présentent un caractère obligatoire à l'inverse de l'annuaire des anciens élèves.

Fiche n°3 : Rôle de la CNIL pour défendre ces principes

La Commission nationale de l'informatique et des libertés, autorité administrative indépendante chargée d'assurer le respect des dispositions de la loi *« Informatique et Libertés »* [(5)] a, à cet égard, deux missions principales :

- informer les personnes concernées de leurs droits et les responsables de traitements de leurs obligations ;
- veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi *« Informatique et Libertés »*.

1. Le contrôle de la conformité à la loi des projets de fichiers et traitements

La CNIL délivre des récépissés pour les déclarations de fichiers qui lui sont adressées, et dispose d'un pouvoir d'autorisation pour les traitements qui, présentent un caractère sensible en raison de leur finalité ou de la nature des données traitées (ex : recours à la biométrie…)

La Commission peut simplifier les formalités déclaratives, voire exonérer de déclaration certains fichiers.

Un mode d'emploi détaillant les procédures existantes est présenté en annexe 1.

La désignation d'un correspondant *« Informatique et Libertés »* entraîne un allègement des formalités préalables (se reporter à la fiche n°4 du guide).

2. Le rôle de conseil et d'information

Le Service d'Orientation et de Renseignement du Public de la CNIL conseille et renseigne les personnes et les organismes qui envisagent de mettre en œuvre des fichiers informatiques, que ce soit au téléphone, par courrier ou par ses publications. Lorsque de nouvelles technologies apparaissent, la CNIL procède à des études, élabore en concertation avec les milieux concernés des recommandations, le cas échéant propose des mesures législatives. Ces activités peuvent également être menées avec ses homologues en particulier européens.

3. L'instruction des plaintes.

La CNIL reçoit les plaintes de toute personne concernant le non-respect de la loi et peut également s'autosaisir. Selon la nature et l'importance des manquements constatés, elle procède au règlement des plaintes soit par voie amiable, soit par la mise en œuvre de son pouvoir de sanction, soit en dénonçant les faits au procureur.

(5) Les textes cités en référence (la loi « Informatique et Libertés », normes simplifiées applicables, délibérations et guides) sont disponibles sur le site web de la CNIL : http://www.cnil.fr.

4. Le pouvoir de contrôle sur place

La CNIL dispose d'un pouvoir de contrôle qui permet à ses membres et ses agents d'accéder à tous les locaux professionnels. Sur place, ses membres et agents peuvent demander communication de tout document nécessaire et en prendre copie, recueillir tout renseignement utile et accéder aux programmes informatiques et aux données.

5. Le pouvoir de sanction

Au titre de son pouvoir de sanction, la CNIL peut :

- adresser des avertissements et des mises en demeure de faire cesser un manquement à la loi ;
- prononcer une injonction de cesser le traitement ou un retrait de l'autorisation et, en cas d'urgence, décider l'interruption du traitement ou le verrouillage des données ;
- prononcer des sanctions pécuniaires pouvant aller jusqu'à 300 000 € en cas de réitération ;
- dénoncer au parquet les infractions à la loi dont elle a connaissance.

Fiche n°4 : Correspondant Informatique et Libertés

Institué à l'occasion de la refonte de la loi « *Informatique et Libertés* », le Correspondant Informatique et Libertés est un acteur et un relais incontournable de la culture « *informatique et libertés* ».

Qu'est-ce que le Correspondant Informatique et Libertés ?

Le Correspondant Informatique et Libertés (CIL) a vocation à être un interlocuteur spécialisé en matière de protection de données à caractère personnel, tant à l'égard du directeur d'établissement, que dans les rapports de ce dernier avec la CNIL. Le CIL occupe ainsi une place centrale dans le développement maîtrisé des nouvelles technologies de l'information et de la communication.

Pourquoi désigner un Correspondant Informatique et Libertés ?

La fonction de correspondant répond à un double objectif.

- Elle entraîne un allègement considérable des formalités auprès de la CNIL. Sa désignation permet en effet d'être exonéré de l'obligation de déclaration préalable des traitements ordinaires et courants. Seuls les traitements identifiés comme sensibles dans la loi demeurent soumis à autorisation et continuent à faire l'objet de formalités.
- Le Correspondant Informatique et Libertés apporte une aide précieuse au directeur d'établissement. Il contribue à une meilleure application de la loi et réduit ainsi les risques juridiques. Il a un rôle de conseil, de veille et d'alerte en matière de déploiement des projets informatiques au sein de l'établissement. Il joue également un rôle essentiel dans la formation et la sensibilisation des personnels de l'établissement aux principes « *informatique et libertés* ».

Quelles sont les compétences requises pour être Correspondant Informatique et Libertés ?

Le CIL peut être un employé de l'établissement ou une personne externe (comme par exemple, un conseiller TICE, un consultant…). La loi a fixé des seuils pour déterminer les cas dans lesquels il est possible de choisir un CIL interne ou externe à l'établissement.

Ainsi, il existe une liberté de choix lorsque moins de 50 personnes sont chargées de la mise en œuvre des traitements ou qui y ont directement accès. Le choix est limité lorsque plus de 50 personnes sont chargées de la mise en œuvre des traitements ou y ont directement accès.

En pratique, pour connaître le seuil applicable, il convient de déterminer le nombre de personnels qui sont chargés :

- du développement et de la maintenance des applications (par exemple, le service informatique) ;

- de la saisie des données ou de la consultation (exemple : service juridique, comptable, ou des ressources humaine).

Le nombre de 50 personnes est apprécié au regard de l'ensemble des applications informatiques mises en œuvre par l'établissement.

Exemple : il est possible de désigner un CIL pour plusieurs établissements dans lesquels plus de 50 personnes sont chargées de la mise en œuvre des traitements ou y ont directement accès. Dans ce cas, le CIL doit être une personne mandatée par un organisme représentant les établissements secondaires.

La plupart des correspondants ont une formation informatique mais ce n'est pas une obligation légale. L'important est qu'il puisse, si nécessaire, bénéficier d'une formation tant technique que juridique, qui soit adaptée à la taille de l'établissement. La CNIL n'a pas à donner d'agrément mais enregistre, la désignation et notifie celle-ci au responsable du traitement.

Quel que soit le choix fait, l'essentiel est qu'il y ait une très bonne collaboration entre le CIL, le RSSI (Responsable de la Sécurité des Systèmes d'Information), le CRI (Centre de Ressources Informatiques) et le service juridique de l'établissement.

Enfin, pour s'acquitter de sa tâche, le Correspondant Informatique et Libertés doit disposer de la liberté d'action et des moyens qui lui permettront de recommander des solutions organisationnelles ou techniques adaptées. Il doit pouvoir exercer pleinement ses missions, en dehors de toute pression, et jouer son rôle auprès du responsable du traitement.

Qui peut désigner un Correspondant Informatique et Libertés ?

Il appartient au chef d'établissement d'exercer un choix.

La désignation d'un correspondant est facultative et traduit l'engagement du responsable du traitement à respecter les dispositions légales.

En pratique : Pour toute information complémentaire sur le correspondant, sa désignation et ses missions, consulter le dossier « *Correspondant* » ou le « *Guide du Correspondant Informatique et Libertés* » sur le site internet de la CNIL. Vous pouvez également contacter le service de la CNIL en charge des correspondants.

Fiche n°5 : Enregistrement et utilisation du numéro de sécurité sociale

De quoi s'agit-il ?

Le NIR, numéro d'inscription au Répertoire National d'Identification des Personnes Physiques (RNIPP), communément appelé numéro de sécurité sociale, est un élément d'identification des personnes physiques. La gestion du NIR est confiée à l'INSEE.

En quoi les libertés sont-elles concernées ?

Le NIR n'est pas un numéro comme les autres.

Il est particulier car il est :

- signifiant – il est composé d'une chaîne de caractères qui permettent de déterminer le sexe, le mois et l'année de naissance, et dans la majorité des cas, le département et la commune de naissance en France ou l'indication d'une naissance à l'étranger ;
- unique et pérenne – un seul numéro est attribué à chaque individu dès sa naissance *a priori* fiable – il est certifié par l'INSEE à partir des données d'état civil transmises par les mairies.

La loi « *Informatique et Libertés* » a toujours soumis à des exigences procédurales particulières l'utilisation du NIR. En effet, les craintes suscitées par la généralisation d'un identifiant national et unique qui rendrait plus aisées les possibilités de rapprochements de fichiers ont conduit le législateur à encadrer strictement l'utilisation de ce numéro.

Que faire ?

Lorsqu'un établissement envisage l'enregistrement et/ou l'utilisation du NIR, il doit tout d'abord s'assurer du fait que cette utilisation est légale.

En effet, l'enregistrement du numéro de sécurité sociale dans un traitement est notamment autorisé :

- dans les fichiers de paie et de gestion du personnel pour l'établissement des bulletins de paie et des différentes déclarations sociales obligatoires (décret n° 91-1404 du 27 décembre 1991) ;
- dans le cadre de la prise en charge des frais de maladie (articles R.115-1 et R.115-2 du code de la sécurité sociale).

Exemple : L'immatriculation des élèves à la sécurité sociale lors de l'inscription dans l'établissement conformément aux dispositions de l'article L.381-4 et L161-14-1 du code de la sécurité sociale pour les élèves inscrits en classe

préparatoire du second degré.

Les états produits et les documents édités ne peuvent donc porter mention de ce numéro que dans le cadre des opérations décrites plus haut.

Cette règle s'applique même dans le cas de logiciels intégrés de gestion et de paie qui doivent être paramétrés pour limiter l'utilisation du numéro de sécurité sociale à ces seules opérations.

En particulier, le numéro de sécurité sociale ne fait pas partie de la liste des informations qui doivent figurer dans le registre unique du personnel, fixée par les articles L.620-3 et R. 620-3 du code du travail, et ne doit donc pas être enregistré dans ce cadre.

Le numéro de sécurité sociale d'un employé ne peut donc pas être utilisé comme numéro de matricule unique pour l'identifier dans tous les fichiers de gestion des ressources humaines de son entreprise ou de son administration.

En dehors des cas évoqués ci-dessus, l'utilisation du numéro de sécurité sociale ne peut être autorisée que dans le cadre d'un décret en Conseil d'Etat ou arrêté pris après avis de la CNIL.

Fiche n°6 : Utilisation de la photographie d'une personne

De quoi s'agit-il ?

L'utilisation de la photographie d'une personne ou d'un groupe de personnes est devenue une pratique courante au sein des établissements scolaires. Elle est, par exemple, apposée sur la carte de l'élève, sur des articles publiés dans une revue ou un journal d'école, sur un site internet, ou encore sur un trombinoscope.

En quoi les libertés sont-elles concernées ?

L'image d'une personne est considérée comme un attribut de sa personnalité ou encore comme un élément de l'intimité de sa vie privée et elle est protégée au titre du droit au respect de la vie privée. Son utilisation en est dès lors strictement encadrée ; en effet, toute personne dispose sur son image et sur l'utilisation qui en est faite, d'un droit exclusif et peut s'opposer à sa reproduction et à sa diffusion dès lors qu'elle n'y a pas préalablement consenti.

Que faire ?

Recueillir l'accord des personnes photographiées

La prise de photographies et leur diffusion doivent s'effectuer dans le respect des règles relatives au droit à l'image.

Toute personne pouvant s'opposer à la reproduction de son image, sur quelque support que ce soit (diffusion de son image sur un intranet, sur internet, etc.), la prise d'une photographie et sa diffusion doivent faire l'objet d'un accord écrit de la personne concernée si elle est majeure ou de ses représentants légaux s'il s'agit d'un élève mineur.

Il appartient donc au responsable de traitement d'obtenir toutes les autorisations utiles préalablement à l'utilisation de photographies.

Exemple de mention à insérer

Il est envisagé de diffuser dans [le journal de l'établissement, le site Internet…] des photos de votre enfant prises à l'occasion des différents événements qui ponctuent la vie de l'établissement. Pour ce faire, nous avons besoin de recueillir votre accord. Nous vous proposons donc de bien vouloir nous signifier si vous acceptez que des photos de vos enfants soient susceptibles d'être diffusées sur le site à l'aide du coupon joint. Nous vous rappelons que vous disposez d'un droit d'accès, de modification, de rectification et de suppression des données qui vous concernent conformément à la loi « *informatique et libertés* » du 6 janvier 1978 modifiée en 2004. Pour exercer ce droit, adressez-vous à [indiquez ici l'adresse où les personnes peuvent exercer leur droit d'accès et de rectification] .

Déclarer auprès de la CNIL

Dès lors qu'elle se rapporte à une personne identifiée ou identifiable, l'image d'une personne est une donnée à caractère personnel. Le traitement informatique de cette donnée (numérisation, diffusion à partir d'un site web, etc.) doit s'effectuer dans le respect de la loi « *Informatique et Libertés* » et donc être déclaré auprès de la CNIL sauf en cas de désignation d'un Correspondant Informatique et Libertés.

Fiche n°7 : Mise en place d'un annuaire des élèves

De quoi s'agit-il ?

La mise en place par une association d'anciens élèves ou par l'établissement lui-même d'un annuaire des élèves est une pratique courante.

En quoi mes libertés sont-elles concernées ?

La création d'un annuaire d'anciens élèves peut, en pratique, soulever des difficultés au regard des principes « *informatique et libertés* » s'agissant plus particulièrement des conditions dans lesquelles il a été constitué et de ses modalités de diffusion (papier, internet).

En effet, la divulgation sur internet du nom et de l'adresse personnelle des anciens élèves sans qu'ils en aient été préalablement informés et mis en mesure de s'y opposer peut comporter un risque pour leur vie privée. Ces informations peuvent, par exemple, être utilisées à leur insu notamment à des fins commerciales.

Que faire ?

Lorsque l'établissement propose un formulaire d'inscription à l'annuaire, celui-ci devra préciser : la finalité de la collecte, à savoir la mise en place d'un annuaire des élèves de l'établissement, son caractère facultatif, les destinataires des données et les modalités d'exercice des droits d'accès, de rectification et d'opposition aux données.

Dans l'hypothèse où l'annuaire serait accessible sur internet, les anciens élèves doivent en être préalablement informés et mis en mesure de s'opposer à la diffusion de leurs coordonnées. Il est recommandé que l'accès à l'annuaire via internet soit strictement réservé aux anciens élèves (exemple : attribution de code d'accès).

Il est également souhaitable que le formulaire d'inscription puisse permettre à l'élève d'indiquer les informations qu'il souhaite ne pas voir diffusées (exemple : son adresse personnelle) tant sur la version web que sur la version papier de l'annuaire. Ces données ne restent alors accessibles qu'au service chargé de la tenue de l'annuaire.

Un ancien élève qui aura été recontacté individuellement (lors d'un événement professionnel par exemple) pourra se voir proposer le formulaire d'inscription à l'annuaire.

Chaque année, un courrier électronique ou postal doit être envoyé à chacun des élèves inscrits sur l'annuaire, leur rappelant les modalités de mise à jour de leurs données personnelles, ainsi que celles de désinscription.

Si ce courrier revient en NPAI (N'habite Plus A l'Adresse Indiquée), toutes les données relatives à cet ancien élève doivent être supprimées.

Il est important également de veiller à insérer une mention légale sur l'annuaire qui précise qu'en aucun cas les données qu'il contient ne peuvent être exploitées à

des fins commerciales ou politiques sauf indication explicite en sens contraire de la personne concernée.

En pratique : Les associations d'anciens élèves

L'établissement scolaire peut communiquer la liste de ses anciens élèves à ces associations dès lors que les intéressés ont, d'une part, été préalablement informés de cette transmission les concernant et ont, d'autre part, eu la possibilité de s'y opposer.

Par ailleurs, l'établissement peut, par voie d'affichage et plus particulièrement lors de la publication des résultats, informer les diplômés de l'existence d'associations d'anciens élèves et des modalités d'inscription via par exemple le site web de l'association.

Fiche n°8 : Enquêtes statistiques portant sur le devenir professionnel et le suivi de cohortes d'élèves

De quoi s'agit-il ?

La mise en place des indicateurs de performances dans le cadre de la LOLF et la nécessité d'adapter au mieux l'offre de formation contribuent au développement d'enquêtes de suivi de cohorte d'élèves. En effet, suivre le parcours des élèves dans le cadre d'un suivi de cohorte est l'occasion d'observer dans la durée le devenir des bacheliers et de mieux comprendre leur orientation.

Le plus souvent, les informations à caractère personnel nécessaires à la réalisation de ce suivi seront extraites de la base de gestion des élèves et peuvent être complétées par des enquêtes auprès des élèves (ex. : connaître pour chaque bachelier, sortant de lycée, son devenir professionnel 18 mois et 3 ans après l'obtention du diplôme).

Les informations recueillies sont ensuite utilisées et analysées dans un but statistique.

En quoi les libertés sont-elles concernées ?

Si la légitimité de ce type d'études ne saurait être remise en question, elles doivent cependant être réalisées dans le respect des droits des personnes (information préalable, droit d'accès, de rectification et d'opposition).

En outre, le risque d'une exploitation des données à des fins autres que celle d'un suivi de cohorte étant toujours possible, une attention particulière doit être apportée aux mesures prises pour assurer la sécurité et la confidentialité de ces traitements et notamment garantir l'anonymat des réponses.

Que faire ?

Les responsables de ces études doivent veiller à la mise en place des mesures suivantes :

- une information préalable des élèves relative à la mise en place de ce type d'études au sein de l'établissement doit être prévue. Celle-ci peut par exemple être réalisée au moment de l'inscription de l'élève ;

- le questionnaire d'enquête adressé aux (anciens) élèves doit :

• rappeler les mentions de la loi *« Informatique et Libertés »* ; celles-ci doivent également figurer sur la lettre d'accompagnement ;

• indiquer qu'il est facultatif et confidentiel ;

• comporter des questions qui restent pertinentes et adaptées au regard de la finalité de l'enquête ;



- une fois l'enquête considérée comme terminée, les informations personnelles détenues par le responsable de l'enquête doivent être détruites ou archivées ; seuls les résultats statistiques peuvent être conservés ;
- les statistiques nécessaires seront réalisées par des personnes habilitées à utiliser la base de gestion des élèves ;
- une information sur l'enquête devra être présentée régulièrement *« au fil de l'eau »* : journal de l'établissement, présentation des résultats lors des *« journées scolarité »*, des réunions d'accueil des anciens élèves…

Se reporter à l'annexe 1 *« Mode d'emploi : comment déclarer ? »* qui précise les cas dans lesquels ces traitements relèvent du régime de la déclaration normale ou de la demande d'autorisation.

Fiche n°9 : Mise en place des espaces numériques de travail (ENT)

De quoi s'agit-il ?

Les Espaces Numériques de Travail (ENT) sont des sites web portail permettant aux élèves, aux enseignants, aux personnels administratifs, d'accéder, via un point d'entrée unique et sécurisé, à un bouquet de services numériques.

- Un accès via internet de son domicile ou à partir des points d'accès disponibles dans chaque établissement ;
- Un accès à des contenus à vocation pédagogique et éducative, une diffusion d'informations administratives ou relatives au fonctionnement de l'établissement, une messagerie électronique, des forums de discussion, etc.

En quoi les libertés sont-elles concernées ?

- Une attention particulière doit être portée aux mesures prises pour assurer la sécurité du dispositif.

En pratique :

Elles doivent notamment garantir que chaque titulaire d'un compte ENT ne puisse accéder qu'aux seules informations le concernant. Exemple : un élève ne peut pas avoir accès aux notes des autres élèves de sa classe.

Il convient de se référer aux annexes « *Sécurités* » du Schéma Directeur des Espaces Numériques de Travail du Ministère en particulier l'annexe « *Authentification, Autorisation, SSO* » qui précise les obligations à respecter en ce qui concerne la politique de gestion des mots de passe (mots de passe non stockés en clair, etc.).

Les responsables d'établissement veillent à sensibiliser les utilisateurs des ENT aux mesures élémentaires de sécurité telles que la confidentialité de leur identifiant de connexion à leur compte ENT.

Que faire ?

- L'information des personnes est essentielle. Chaque responsable d'établissement se doit d'informer les utilisateurs des ENT de leurs droits au regard de la loi « *Informatique et Libertés* ».

En pratique :

Cette information doit être prévue sur la page d'accueil du portail ENT et lors de la phase de création d'un compte ENT.
Modèle de mention d'information : Cet espace numérique de travail (ENT) propose des contenus à vocation pédagogique et diffuse des informations administratives ou relatives à la vie scolaire. Chaque utilisateur ne peut accéder qu'aux seules informations auxquelles il a besoin d'accéder dans l'exercice de ses fonctions au sein de l'établissement. Conformément à la loi « *Informatique et Libertés* », vous disposez d'un droit d'accès, de rectification et d'opposition aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir



communication des informations vous concernant, veuillez vous adresser à : [indiquez-ici le service. Préciser adresse postale et adresse électronique].

• Les formalités auprès de la CNIL

- Qui doit déclarer ?

Le directeur de l'établissement qui a décidé de la mise en œuvre d'un ENT au sein de son établissement.

- Comment déclarer ?

Les ENT sont considérés comme des téléservices de l'administration électronique. Par conséquent, le traitement relève du régime de la demande d'avis.

Une procédure de déclaration simplifiée est prévue à condition que le dispositif ENT respecte le cadre fixé par l'arrêté du 30 novembre 2006 pris après avis de la CNIL[6], à savoir notamment les finalités, les droits des personnes et les mesures de sécurité nécessaires à la protection des données à caractère personnel.

(6) cf. Délibération n° 2006-104 adoptée par la CNIL le 27 avril 2006 portant avis sur la mise en place des espaces numériques de travail (ENT) au sein des établissements scolaires et universitaires.

Fiche n°10 : Contrôle de l'utilisation des moyens informatiques

Afin d'assurer la sécurité de leur réseau et/ou de leurs ressources informatiques, les établissements peuvent être conduits à mettre en place des instruments pour contrôler l'utilisation des outils informatiques mis à disposition de leurs élèves et de leurs personnels [(7)].

Ce contrôle est légitime dès lors qu'il est réalisé de manière transparente, à savoir avec une parfaite information des utilisateurs. La rédaction d'une Charte d'utilisation des outils informatiques est particulièrement utile pour rappeler les obligations mutuelles de l'établissement et de l'utilisateur, définir les modalités des contrôles qui peuvent être effectués et les sanctions auxquelles s'expose l'utilisateur s'il ne respecte pas les règles d'utilisation.

La présente fiche se propose d'aborder plus particulièrement les questions relatives à l'utilisation de la messagerie électronique et de l'internet par les personnels de l'établissement sur le lieu de travail. Pour toute information complémentaire sur ce sujet, consulter le *« Guide pratique pour les employeurs »* sur le site internet de la CNIL.

1. Le contrôle de l'utilisation de la messagerie électronique professionnelle

De quoi s'agit-il ?

L'utilisation de la messagerie électronique professionnelle pour envoyer ou recevoir, dans des proportions raisonnables, des messages à caractère personnel correspond à un usage généralement et socialement admis.

Il est possible de l'interdire, mais, même dans un tel cas, la nature d'une correspondance privée est protégée par *« le secret des correspondances »* dans le respect de la loi et de l'état actuel de la jurisprudence.

En quoi les libertés sont-elles concernées ?

La surveillance des courriers d'un agent par sa direction doit respecter les principes issus du droit à la vie privée, même dans le cadre de la vie professionnelle. En effet, la mise en œuvre d'outils de contrôle doit s'opérer dans le respect du principe consacré à l'article 8 de la Convention européenne des droits de l'homme selon lequel : *« Le salarié a droit, même au temps et lieu de travail, au respect de l'intimité de sa vie privée ».*

7 Ce contrôle est notamment réalisé à partir de la conservation de données techniques appelées données de connexion ou données relatives au trafic (ex. : adresses URL visitées, adresse IP). On sait qu'il se pose la question de savoir si les établissements scolaires offrant un accès à Internet à leurs étudiants sont soumis aux dispositions de l'article L.34-1 du code des postes et des communications électroniques. Selon cet article, les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ont l'obligation de conserver les données de connexion des personnes utilisatrices de leurs services. En tout état de cause, il convient de rappeler que cette disposition n'impose pas d'identifier les élèves par la tenue par exemple d'un fichier des utilisateurs.



Que faire ?

C’est la jurisprudence qui a défini les conditions dans lesquelles un employeur peut contrôler l’utilisation de la messagerie professionnelle de ses employés.

Ainsi, un arrêt de la Cour de cassation de 2001 a consacré le droit des salariés au respect de l’intimité de leur vie privée avec une interdiction pour l’employeur de prendre connaissance du contenu des correspondances qui relèveraient de la vie privée des personnes via la messagerie électronique professionnelle.

Toutefois, en 2005, la Cour de cassation a reconnu à l’employeur le droit, dans certains cas, d’accéder aux fichiers personnels d’un salarié enregistrés sur le disque dur de son poste de travail. Elle pose le principe que, désormais, la nature personnelle d’un fichier ne suffit plus à le soustraire à un contrôle de l’employeur mais définit étroitement les conditions d’un tel contrôle.

Ainsi :

- par principe, l’accès à l’espace réservé à l’employé nécessite la prévision d’un tel accès dans le règlement intérieur ainsi que l’information préalable du salarié (qui doit être présent ou au moins être prévenu) ;
- par exception, le contrôle de l’espace réservé est possible sans inscription au règlement intérieur et sans information préalable en cas de « *risque ou d’événement particulier* ».

• Identifier ses messages personnels

Il appartient à l’employé :

- de classer systématiquement le message dans un dossier « *personnel* » *;*
- d’indiquer dans l’objet du message la mention « *personnel* » *;*

• Informer les personnes

Il est recommandé que la direction de l’établissement informe ses personnels au sujet :

- de l’existence de procédures de contrôles quant à l’utilisation de la messagerie électronique ; cette information peut être assurée par l’envoi à chaque agent d’un courrier électronique dans lequel doivent être rappelées les mentions « *informatique et libertés* ». Cette information peut être utilement complétée par voie d’affichage ;
- des procédures de surveillance et d’archivage mises en œuvre pour des raisons de sécurité des systèmes d’information (ex. : encombrement du réseau);
- de la durée de conservation des données dans le cas de mesures d’archivage ;

(8) COUR DE CASSATION, Chambre sociale, 17 mai 2005, Philippe X. c/ Société Cathnet-Science, N° 03-40.017 / arrêt n° 1089 – Cassation

- de l'existence et la date de la consultation préalable des instances représentatives du personnel.

• **Rappeler les prérogatives et les obligations des administrateurs réseaux**

- Prérogatives : accès à l'ensemble des données y compris celles qui sont sur le disque dur du poste de travail pour pouvoir travailler efficacement ; utilisation de logiciels de télémaintenance (détection de pannes ou prise de contrôle à distance [9]) ;

- Obligations : l'accès aux données enregistrées par les employés (dont les correspondances personnelles) ne peut être justifié que dans le cas d'un dysfonctionnement important ; obligation de confidentialité à rappeler dans leur contrat et dans la charte d'utilisation des ressources informatiques. Respect de la durée de conservation des données indiquée dans le dossier de déclaration CNIL ou dans le registre du CIL (Correspondant Informatique et Libertés) ; en l'espèce, une durée de 6 mois à 1 an paraît raisonnable et suffisante.

Les usagers doivent être informés des prérogatives des administrateurs du réseau.

• **Déclarer à la CNIL**

La mise en place d'un contrôle de la messagerie (nombre de mails entrants et sortants par employé, identification de l'émetteur et des destinataires des envois de mails, taille des fichiers transmis en pièces jointes, outil d'archivage des messages échangés…) constitue un traitement de données à caractère personnel et doit par conséquence être déclaré à la CNIL sauf en cas de désignation d'un CIL.

A noter :

Accès aux données informatiques en cas d'absence d'un employé

L'obligation de loyauté impose à l'employé absent de son poste de travail de communiquer à l'employeur qui en fait la demande tout document nécessaire à la poursuite de l'activité de l'établissement. Pour autant, les modalités d'accès de l'employeur aux données stockées sur l'environnement informatique d'un employé absent (messagerie, fichiers, supports de stockage) devraient être préalablement définies en concertation et diffusées auprès de l'ensemble des employés susceptibles d'être concernés (via une charte par exemple).

2. Le contrôle de l'utilisation d'internet

De quoi s'agit-il ?

Une interdiction générale et absolue de toute utilisation d'internet à des fins autres que professionnelles ne paraît pas réaliste dans une société de

(9) Les logiciels de télémaintenance ou de prise de main à distance ne peuvent être utilisés par l'employeur à des fins de contrôle de l'activité de ses personnels.



l'information et de la communication. Elle semble de plus disproportionnée au regard des textes applicables et de leur interprétation par la jurisprudence.

Un usage raisonnable du personnel, non susceptible d'amoindrir les conditions d'accès professionnel au réseau ne mettant pas en cause la productivité est généralement et socialement admis par la plupart des établissements.

Que faire ?

• Rédiger une « charte » d'utilisation d'internet au sein de l'établissement

Celle-ci peut notamment prévoir :

- la mise en place de dispositifs de filtrage de sites non autorisés, associés au pare-feu (sites diffusant des produits à caractère pornographique, pédophile, incitant à la haine raciale, révisionniste, etc.) comme une mesure de prévention ;
- l'interdiction de télécharger des logiciels, de se connecter à un forum ou d'utiliser le *«chat»*, d'accéder à une boîte aux lettres personnelle par internet compte tenu des risques de virus.

• Informer les personnes

Les modalités d'un tel contrôle de l'usage d'internet doivent faire l'objet d'une consultation des instances représentatives du personnel et d'une information des utilisateurs et des élèves en particulier, y compris lorsque le contrôle est dépourvu d'un caractère directement nominatif.

• Déclarer auprès de la CNIL

Un contrôle *a posteriori* des données de connexion à internet, restitué de façon globale, par exemple au niveau de l'organisme ou d'un service déterminé, devrait dans la plupart des cas être suffisant sans qu'il soit nécessaire de procéder à un contrôle individualisé des sites visités par un employé déterminé.

Toutefois, si l'établissement met en place un dispositif de contrôle individuel des employés destiné à produire, poste par poste, un relevé des durées de connexion ou des sites visités, le traitement automatisé de données à caractère personnel ainsi mis en œuvre doit être déclaré à la CNIL (sauf désignation d'un Correspondant Informatique et Libertés).

La durée pendant laquelle les relevés ainsi établis sont conservés doit être précisée. Une durée de conservation de l'ordre de six mois devrait être suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet. Le dossier de déclaration doit en outre comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées sur de tels dispositifs.



Fiche n°11 : Diffusion des résultats d'examens et des notes

De quoi s'agit-il ?

Comme le précise une circulaire ministérielle, les résultats des examens sont portés à la connaissance des étudiants par voie d'affichage[(10)]. Traditionnellement, cette proclamation des résultats est réalisée par le biais d'un affichage dans les locaux de l'établissement. Cette publicité ne s'applique pas aux notes obtenues qui sont communiquées individuellement à chaque élève.

Il est désormais fréquent que les établissements scolaires permettent à leurs élèves d'accéder à leurs résultats d'examen et à leurs notes via internet.

En quoi les libertés sont-elles concernées ?

La diffusion des résultats d'examen et des notes des élèves via internet est susceptible de porter atteinte à la vie privée des personnes compte tenu des caractéristiques propres au réseau internet qui est par principe un réseau ouvert au public. En effet, ces informations peuvent être captées et utilisées par des tiers dès lors qu'elles sont diffusées sur le réseau.

Que faire ?

• Informer les élèves de la diffusion sur internet

S'agissant de la publicité des résultats d'examen sur internet et en l'absence de règles définissant les modalités de diffusion des résultats des examens, il est recommandé que les élèves aient été préalablement informés d'une telle diffusion et mis en mesure de s'y opposer. Cette information peut, par exemple, être prévue sur le dossier d'inscription de l'élève.

En pratique : Les mentions d'information sur le dossier d'inscription de l'élève doivent permettre aux candidats de s'opposer d'une part à la diffusion de leurs résultats sur internet, d'autre part à la communication d'informations les concernant à des tiers.

S'agissant de la mise en ligne des notes d'examen, chaque personne concernée doit disposer d'un code d'accès et d'un mot de passe (accès restreint) pour les obtenir. L'accès aux notes, qui sont des données personnelles, est en effet strictement personnel. Le plus souvent, cet accès est réalisé via le compte ENT de l'élève.

• Déclarer auprès de la CNIL

L'accès aux résultats d'examen et aux notes via internet par le biais d'identifiants de connexion doit être considéré comme un téléservice de l'administration électronique. Sa mise en œuvre est par conséquent soumise à avis préalable de la CNIL. Si cet accès est envisagé dans le cadre d'un ENT, il peut être déclaré sous une forme simplifiée à condition que le dispositif ENT respecte le cadre fixé par l'arrêté du 30 novembre 2006[(11)].

(10) Circulaire ministérielle n°2000-033 du 1er mars 2000.
(11) Cf. Annexe 1 : Comment déclarer ? Et Fiche 12 du guide sur les Espaces Numériques de Travail.



En pratique :

A quel moment la diffusion des résultats d'examen par les sociétés privées doit-elle intervenir ?

Un avis de la Commission d'accès aux documents administratifs (CADA) a précisé que la publicité des résultats d'examen par les rectorats devait se faire de manière simultanée avec la transmission de ces résultats aux sociétés privées. Cet avis précise que cette communication doit être réalisée au moment même où les résultats sont rendus publics. Ces sociétés privées ne peuvent donc pas publier les résultats avant le ministère de l'éducation nationale.

Peut-on s'opposer à la transmission à des sociétés privées de ses résultats d'examen ?

Lors de l'inscription de l'élève dans l'établissement, le consentement du représentant légal devra être recueilli dans un formulaire qui peut être joint au dossier d'inscription. Le représentant légal a donc bien la possibilité de s'opposer à cette transmission. Une case à cocher spécifique pourra être prévue.

Peut-on s'opposer à la diffusion dans la presse de ses résultats d'examen ?

Le représentant légal a également la possibilité de s'opposer à cette transmission au moment de l'inscription. Une case à cocher spécifique pourra être prévue.

Fiche n°12 : Communication à des tiers autorisés d'informations relatives aux personnels et aux élèves

De quoi s'agit-il ?

La loi permet à des autorités publiques de se faire communiquer, dans le cadre de leurs missions et sous certaines conditions, des informations issues de fichiers. Il s'agit du cas des *« tiers autorisés ».*

En quoi les libertés sont-elles concernées ?

Certaines administrations sont autorisées par la loi à se faire communiquer ponctuellement des informations afin d'assurer leurs missions d'intérêt général.

Afin de protéger les libertés, il revient à l'établissement de s'assurer que le demandeur correspond bien à l'un de ceux qui sont autorisés.

Le fait, pour un responsable du traitement, de porter à la connaissance d'un tiers qui n'a pas qualité pour les recevoir des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée constitue une infraction pénale punie de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Que faire ?

De façon générale, l'établissement ne peut (sauf cas des tiers autorisés prévus par la loi), communiquer à des tiers des informations nominatives relatives à ses personnels et/ou aux représentant légaux des élèves mineurs, aux élèves majeurs. Ces derniers doivent être préalablement informés et en mesure de s'y opposer dans certains cas.

- **Dans quelles conditions un établissement peut-il communiquer à des *« tiers autorisés »* des renseignements sur ses personnels et ses étudiants ?**

Cette communication ne peut être effectuée que sur demande ponctuelle écrite, visant des personnes nommément désignées, identifiées directement ou indirectement. Il est exclu qu'elle porte sur l'intégralité d'un fichier. L'établissement n'est pas tenu de répondre à une simple demande téléphonique qui ne lui permettra pas de s'assurer de la qualité de son interlocuteur.

La demande doit être formulée par écrit et préciser le texte législatif fondant ce droit de communication, ainsi que les catégories d'informations sollicitées. L'établissement doit s'assurer de sa conformité aux textes invoqués et peut toujours, en cas de doute, interroger la CNIL.

- **Quels sont les tiers autorisés à obtenir ponctuellement des informations personnelles détenues par les établissements ?**

a) L'administration fiscale

- Le Trésor public (direction générale de la comptabilité publique uniquement dans les conditions fixées par les articles L.81 à L.95 du Livre des Procédures fiscales pour le recouvrement de créances fiscales ou des amendes et condamnations pécuniaires).
- La direction générale des impôts ou la direction générale des douanes en vue de l'établissement de l'assiette, du contrôle, du recouvrement des impôts (articles L. 81 à L. 95 du Livre des procédures fiscales).

b) Les organismes sociaux

- Les organismes débiteurs de prestations familiales ou en charge du versement du RSA dans les conditions prévues par l'article L.583-3 du code de la sécurité sociale.
- Les organismes débiteurs de prestations familiales ou les huissiers de justice au titre de leur mission de recouvrement des créances alimentaires impayées (article 7 de la loi n° 73-5 du 2 janvier 1973).

c) Les administrations de la justice, de la police et de la gendarmerie

- Les magistrats, dans le cadre des dispositions des codes de procédure pénale et de procédure civile (notamment les articles 56, 57, 92 à 97 du code de procédure pénale).
- Le procureur de la République, à la demande de l'huissier de justice porteur d'un titre exécutoire et au vu d'un relevé certifié sincère des recherches infructueuses qu'il a tentées pour l'exécution (article 40 de la loi n° 91-650 du 9 juillet 1991).
- Les officiers de police judiciaire de la police et de la gendarmerie nationales agissant en flagrant délit, sur commission rogatoire ou dans le cadre d'une enquête préliminaire (articles 57-1, 60-1 et 76-3 du code de procédure pénale) y compris par voie informatique ou télématique (article 60-2 du même code).
- Les bureaux d'aide judiciaire afin de demander la vérification des ressources en vue de l'attribution de l'aide judiciaire (loi n° 72-11 du 3 janvier 1972 modifiée par la loi du 31 décembre 1982 relative à l'aide judiciaire).



d) Les autres administrations bénéficiant d'un droit de communication

- Les services déconcentrés du travail et de l'emploi dans le cadre du contrôle de la recherche d'emploi (ordonnance n°86-1286 du 20 décembre 1986, articles L. 351-1 et R. 351-32 du code du travail).

- Les services en charge de la gestion des allocations supplémentaires prévues aux articles L 815-2 et 3 du code de la sécurité sociale (fonds de solidarité vieillesse et fonds spécial d'invalidité) pour le recouvrement sur la succession des héritiers (articles L. 815-12 et L. 815-15 du code de la sécurité sociale).

Fiche n°13 : Conditions d'accès des collectivités locales aux fichiers d'élèves

L'accès des collectivités locales aux fichiers d'élèves est dans certains cas autorisé par des textes législatifs et réglementaires. Si la communication de ces données ne repose sur aucun fondement juridique, elle doit être effectuée, en application de la loi informatique et libertés, après information des personnes concernées qui peuvent ainsi s'opposer, si elles le souhaitent à cette transmission.

Le ministère de l'éducation nationale a créé, par un arrêté du 22 septembre 1995 pris après avis n°95-098 de la CNIL, un système d'information dénommé SCOLARITE. Il a pour objet d'assurer la gestion administrative et pédagogique des élèves par les établissements publics du second degré. Ce traitement doit aussi permettre la gestion académique et l'établissement de statistiques par les rectorats et les inspections académiques ainsi que la gestion prévisionnelle et la mise en œuvre d'études statistiques par l'administration centrale.

Cette application est implantée dans tous les établissements publics du second degré et dans les établissements privés qui ont adhéré au système.

Le système SCOLARITE est ainsi articulé autour de trois bases de données : une base des élèves au niveau de l'établissement (BEE), une base des élèves au niveau académique (BEA), une base centrale de pilotage (BCP) de l'administration centrale.

L'arrêté du 22 septembre 1995 énumère pour chaque base les données enregistrées et leurs destinataires. Ainsi, son article 7a fixe les règles de transmission aux collectivités territoriales des données sur les élèves gérées par l'établissement d'enseignement.

A noter : Le ministère de l'éducation nationale a saisi en 2006 la CNIL d'une déclaration de modification du traitement « *SCOLARITE* » afin de permettre l'accès par les conseils généraux et régionaux aux fichiers d'élèves détenus par les rectorats. Ainsi les conseils généraux dans le cadre de leurs compétences en matière de sectorisation scolaire (cf. dispositions de la loi du 13 août 2004 relative aux libertés et responsabilités locales) peuvent être destinataires des données suivantes : l'année de rentrée scolaire, le numéro d'établissement de l'année en cours et de l'année précédente, l'adresse de l'élève et la classe et le niveau de sectorisation. Ils peuvent également être destinataires ainsi que les conseils régionaux des données concernant les élèves leur permettant l'octroi des aides à la scolarité (attribution d'équipements informatiques ou d'aides diverses). Dans ce cas, cette transmission est subordonnée à la diffusion d'une information préalable permettant aux personnes concernées de s'y opposer.

En pratique : A quelles conditions un maire peut-il constituer un fichier des enfants scolarisés ?

Le maire doit procéder chaque année au recensement des enfants résidant dans sa commune et qui sont soumis à l'obligation d'assiduité scolaire. La loi du 5 mars 2007 (art. L.131-6 du Code de l'éducation) sur la prévention de la délinquance lui permet de mettre en œuvre un traitement de données à caractère personnel concernant les enfants en âge scolaire domiciliés dans la commune sur la base des informations que lui transmettent les organismes chargés du versement des prestations familiales, les chefs d'établissement scolaire et l'inspecteur d'académie. Le maire a ainsi connaissance des informations sur le défaut d'assiduité scolaire des élèves. Ce traitement doit faire l'objet d'une déclaration à la CNIL, sauf si un CIL a été désigné. S'il comporte des appréciations sur les difficultés sociales des personnes, il devra faire l'objet d'une demande d'autorisation. Les familles concernées doivent être informées des modalités de mise en œuvre du traitement

Fiche n°14 : Utilisation de la biométrie

De quoi s'agit-il ?

La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales (contours ou forme de la main ou du visage, dessins de l'iris, empreinte digitale ou palmaire, ADN etc.). Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles sont, pour la plupart, uniques et permanentes.

La biométrie est principalement utilisée pour renforcer la sécurité des accès à des locaux.

En quoi les libertés sont-elles concernées ?

Du fait des dangers potentiels liés à l'exploitation de ces caractéristiques physiques, qui sont propres à chaque être humain et dont certaines (empreintes digitales, ADN…) peuvent être collectées à l'insu des intéressés, les traitements faisant appel à un dispositif biométrique sont soumis par la loi à un régime d'autorisation préalable de la CNIL.

Que faire ?

D'une manière générale, il existe deux types de procédures pour notifier à la CNIL l'utilisation d'applications biométriques. La détermination de la procédure applicable est essentiellement fonction de la biométrie choisie, ainsi que du contexte d'utilisation.

1) La procédure d'autorisation au cas par cas pour les dispositifs biométriques :

- Reposant sur un enregistrement de l'empreinte digitale dans une base de données centralisée ou dans le lecteur.

Ils doivent être justifiés par l'existence d'un fort impératif de sécurité.

- Reposant sur des caractéristiques biométriques telles que le visage, l'iris ou la voix.

Exemple : Le contrôle de l'accès aux locaux sensibles où sont conservés les sujets nationaux d'examens.

2) L'autorisation unique n° 9 :

Elle concerne les dispositifs biométriques utilisant la technologie de la reconnaissance du contour de la main pour des systèmes de contrôle d'accès aux restaurants scolaires. Les données enregistrées sont limitativement énumérées par l'autorisation unique. Seules peuvent être enregistrées les données de gestion utiles pour l'accès au restaurant et les gabarits biométriques de la main associés à un code d'accès personnel. Les données relatives à l'identité des élèves et des personnels sont conservées pendant la durée de

leur scolarité dans l'établissement pour les premiers et pendant la durée de leur affectation au sein de l'établissement pour les seconds.

Comment déclarer ?

Si le traitement est strictement conforme à cette autorisation unique, une simple déclaration de conformité suffit. Elle peut être effectuée en ligne, à partir du site web de la CNIL. Cette formalité est requise y compris si l'établissement a désigné un Correspondant Informatique et Libertés.

Si le traitement n'est pas conforme à l'autorisation unique n°9, les établissements y compris ceux ayant désigné un Correspondant Informatique et Libertés, doivent adresser à la CNIL une demande d'autorisation.

Attention ! La norme simplifiée n° 42, relative à la gestion des contrôles d'accès aux locaux, des horaires et de la restauration n'est pas applicable aux applications faisant appel à un procédé de reconnaissance biométrique.

Fiche n°15 : Dispositifs de vidéosurveillance

De quoi s'agit-il ?

La vidéosurveillance consiste à placer des caméras de surveillance dans un lieu public ou privé, pour prévenir des actes de malveillance. Elles peuvent être fixes ou mobiles, automatiques ou télécommandées.

En quoi les libertés sont-elles concernées ?

Les systèmes de vidéosurveillance peuvent intrinsèquement porter atteinte aux libertés individuelles (par exemple, à la liberté d'aller et venir). Il est dès lors nécessaire d'accompagner leur mise en œuvre d'un certain nombre de garanties.

Que faire ?

1) Une réflexion préalable indispensable

Une réflexion préalable à la décision d'utiliser un système de vidéosurveillance, comportant notamment une analyse précise des risques tenant compte des incidents survenus dans l'enceinte de l'établissement devrait être menée. Elle peut permettre d'identifier les solutions alternatives pour atteindre l'objectif poursuivi sans recourir à ce moyen (une sécurisation des accès aux moyens de badges magnétiques, surveillance renforcée par les personnels, une modification des heures d'ouvertures de certaines issues peuvent par exemple constituer des réponses efficaces et adaptées à un objectif particulier de sécurisation).

2) Le nécessaire respect du principe de proportionnalité

Si le déploiement de tels dispositifs répond généralement à un objectif sécuritaire (contrôle des accès aux locaux), il ne peut avoir pour objectif la mise sous surveillance spécifique d'un employé déterminé ou d'un groupe particulier de personnes. Le nombre, l'emplacement, l'orientation, les fonctionnalités et les périodes de fonctionnement des caméras, ou la nature des tâches accomplies par les personnes devant être soumises à la vidéosurveillance, sont autant d'éléments à prendre en compte lors de l'évaluation du caractère proportionné du système.

Exemples : Certains systèmes de vidéosurveillance sont susceptibles de présenter un caractère illégal :

- un système installé dans un lieu susceptible de porter atteinte à l'intimité de la vie privée des personnes (vestiaires, douches, toilettes) ;
- un système installé de façon à enregistrer de façon spécifique les allées et venues des personnes se rendant dans un local syndical.

3) L'obligation d'information

Il ne doit pas y avoir de surveillance à l'insu des personnes concernées à savoir

des enseignants, des élèves, des personnels et des visiteurs.

L'existence d'un système de vidéosurveillance doit être portée à la connaissance de toute personne filmée ou susceptible de l'être, de façon claire et permanente, par exemple au moyen de panonceaux apposés à l'entrée des locaux (exemple fourni ci-dessous).

Exemple de mentions d'information à diffuser

Établissement sous vidéosurveillance

Nous vous informons que cet établissement est placé sous vidéosurveillance pour des raisons de … [indiquer les finalités poursuivies]. Pour tout renseignement, s'adresser au service … ou à … [identifier la personne ou le service compétent], auprès duquel vous pouvez également exercer votre droit d'accès, conformément à la loi « *Informatique et Libertés* ».

Les instances représentatives du personnel doivent être consultées avant toute mise en œuvre d'un système de vidéosurveillance et précisément informées des fonctionnalités envisagées.

4) L'élaboration d'un document de référence

Il est recommandé d'établir un document identifiant clairement les objectifs et les modalités d'utilisation du système de vidéosurveillance, les personnes habilitées et formées à visionner les images, la durée maximale de leur conservation et les modalités d'exercice du droit d'accès aux images.

5) Une visualisation des images restreinte aux seuls destinataires habilités

Les images enregistrées ne peuvent être visionnées que par les seules personnes dûment habilitées à cet effet, dans le cadre de leurs attributions respectives (par exemple : le responsable de la sécurité de l'établissement). Ces personnes devraient être particulièrement formées et avoir été sensibilisées aux règles encadrant la mise en œuvre d'un système de vidéosurveillance.

6) Une durée de conservation des images limitée

Sauf enquête ou information judiciaire, la durée de conservation des images enregistrées à l'aide d'un dispositif de vidéosurveillance ne devrait pas excéder quelques jours et les enregistrements doivent être détruits par la suite. Cette durée ne peut en tout état de cause s'étendre au delà d'un mois.

7) La nécessité d'accomplir certaines formalités préalables

Un système de vidéosurveillance numérique ne peut être installé que s'il a préalablement fait l'objet d'une déclaration auprès de la CNIL. Celle-ci précisera notamment les justifications particulières qui ont conduit à l'installation d'un dispositif de vidéosurveillance. Le traitement est toutefois dispensé de déclaration en cas de désignation d'un Correspondant Informatique et Libertés.

Attention ! L'installation d'un système de vidéosurveillance sur la voie publique



ou dans un lieu ouvert au public [12] est subordonnée à l'obtention d'une autorisation préfectorale.

Exemple :

Le système est implanté sur la voie publique pour filmer les abords de l'établissement scolaire.

Attention ! Si le système prévu devait s'accompagner d'un dispositif de reconnaissance faciale, il devrait alors faire l'objet d'une demande d'autorisation à la CNIL dans la mesure où il fait appel à une technique biométrique [13].

(12) Il appartiendra à chaque établissement de déterminer si le système de vidéosurveillance est installé dans un lieu ouvert au public et donc soumis à autorisation préfectorale, en fonction des délimitations physiques ou matérielles (clôtures, contrôles d'accès,…). Sur ce point précis, la circulaire du 12 mars 2009 relative à l'application de l'article 10 de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité indique que, selon la jurisprudence, un lieu public est « un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions ».

(13) Se reporter à la fiche sur la biométrie.



Fiche n°16 : Commission locale Informatique et Libertés (CLIL)

Le rôle de la CLIL

La Commission nationale de l'informatique et des libertés encourage la création dans des établissements d'enseignement secondaire de commissions locales informatique et libertés (CLIL).

La CLIL a vocation a être un lieu d'échanges et de discussions au sein de l'établissement d'enseignement pour tout ce qui concerne l'utilisation des technologies de l'information et de la communication : expliciter les enjeux, présenter les risques, informer sur les droits des personnes en ce qui concerne tout particulièrement la protection des données à caractère personnel.

La CLIL a non seulement pour objet de relayer les recommandations et décisions de la CNIL auprès des élèves, parents et éducateurs, mais également d'informer la CNIL des problèmes et besoins rencontrés sur le terrain ou de toute initiative intéressant les thèmes *« informatique et libertés »* et qui nécessiterait une prise de position officielle de la CNIL. Elle a donc un rôle pédagogique et civique en permettant de diffuser la culture Informatique et Libertés.

Les modalités pratiques de mise en place

La création d'une CLIL repose sur la volonté du responsable de l'établissement et de son équipe. Il leur appartient de décider de sa mise en place, la décision formelle étant prise par le conseil d'administration de l'établissement. Une fois la mise en place de la commission locale effective, le chef d'établissement doit en informer la CNIL par un courrier adressé au président.

La composition de la CLIL

Il convient de tenir compte de l'importance de l'établissement pour fixer le nombre de représentants de l'administration, des personnels, des élèves et des parents. Au nombre des membres de droit, outre le proviseur, devrait figurer l'administrateur du réseau informatique. Le correspondant informatique et libertés peut être chargé d'animer cette commission.

En fonction des thèmes abordés lors des réunions, des experts peuvent être sollicités. Le conseiller TICE (conseiller pour les technologies de l'information et de la communication) du rectorat peut être un interlocuteur important de ce point de vue.

Les relations CNIL-CLIL

Les CLIL disposent d'un interlocuteur privilégié auprès du service du correspondant informatique et libertés de la CNIL, auquel elles peuvent adresser un compte rendu de leurs réunions afin de faire remonter tout problème relevant



de sa compétence. La CNIL, de son côté, met en relation des établissements rencontrant les mêmes difficultés ou les mêmes besoins ou ayant résolu des problèmes particuliers, afin de favoriser les échanges et un dialogue constructif.

Exemple :

La CLIL de l'Académie de Nancy-Metz

En juin 2006, l'académie de Nancy-Metz a créé une CLIL dans le cadre du projet régional d'intégration de services numériques pour l'éducation (Prisme). Cette commission a notamment pour objet de définir une charte du bon usage d'un espace numérique de travail (ENT).

La mise en place d'une Commission locale informatique et libertés n'est pas définie par la loi, elle obéit à des modalités souples, la Commission est extrêmement favorable à de telles initiatives.

La collaboration entre la CNIL et les établissements scolaires peut également prendre la forme d'une convention de partenariat définissant des axes de collaboration en vue d'améliorer la connaissance et la diffusion de la culture Informatique et libertés auprès des élèves, des enseignants et des personnels administratifs.

Fiche n°17 : Création de sites internet

Des sites web peuvent être créés dans le cadre d'activités au sein de l'établissement scolaire comme par exemple le site web du lycée ou celui d'une association d'élèves.

En quoi mes libertés sont-elles concernées ?

Du fait de sa mise en ligne sur le réseau internet, un site web constitue un espace ouvert au public. Aussi, la diffusion de données à caractère personnel sur ces sites est-elle susceptible de porter atteinte à la vie privée des personnes dès lors qu'elles n'ont pas été préalablement informées d'une telle diffusion.

De plus, l'existence de moteurs de recherche de plus en plus performants multiplie les risques en matière d'atteinte à la vie privée. En effet, l'utilisation des moteurs de recherche à partir du nom d'une personne permet d'accéder à l'ensemble des pages web où est diffusé ce nom (possibilité de reconstituer une « *biographie* » virtuelle des personnes - utilisation par des employeurs par exemple dans le cadre d'une embauche).

Exemple : La CNIL a ainsi veillé à ce que certaines sanctions disciplinaires du ministère de l'Education nationale ne soient accessibles qu'aux seules personnes qui avaient à en connaitre, et non plus diffusées à partir des sites web des ministères concernés auxquels chacun peut avoir accès.

Que faire ?

La mise en ligne d'un site web, que celle-ci soit effectuée dans un cadre privé ou professionnel, doit s'effectuer dans le respect d'un certain nombre de règles. Ainsi par exemple, la diffusion de propos diffamatoires, d'injures ou propos racistes sur un site peut être pénalement sanctionnée. Des sanctions disciplinaires pourraient également être prononcées à l'encontre d'un élève qui aurait tenu sur son « *blog* » des propos calomnieux ou injurieux à l'égard du corps enseignant et administratif de son établissement.

Enfin, dès lors qu'un site web diffuse ou collecte des données à caractère personnel, celui-ci est soumis au respect des dispositions de la loi « *Informatique et Libertés* ».

En pratique : Les sites web personnels (« *blogs* ») n'ont pas à être déclarés auprès de la CNIL (dispense adoptée par la CNIL en 2005).

Attention ! La diffusion et la collecte de données à caractère personnel opérées à partir d'un site web dans le cadre d'activités professionnelles, politiques, ou associatives restent soumises à l'accomplissement des formalités préalables prévues par la loi.

En ce qui concerne les sites web qui ne seraient pas créés dans le cadre d'une activité exclusivement personnelle, comme par exemple le site institutionnel du lycée, ils sont également soumis aux dispositions de la loi « *Informatique et Libertés* ».



Ainsi, par exemple :

- lors de la collecte de données à caractère personnel (ex. : abonnement à la lettre d'information), les personnes auprès desquelles sont recueillies les informations doivent être informées de la finalité de cette collecte, des destinataires ou catégories de destinataires des données et de l'existence d'un droit d'accès, de rectification et d'opposition (se reporter à l'annexe 3 pour un modèle de mention d'information)
- la diffusion de la photographie des élèves et des personnels sur ce site est subordonnée au recueil du consentement des personnes concernées.

Fiche n°18 : Les obligations du blogueur

De quoi s'agit-il ?

Plus connu sous le nom de « *blogs* », les sites personnels ont pour vocation la diffusion d'informations à destination du cercle familial ou des proches, la mise en ligne d'un journal personnel (blocs-notes ou « *blog* ») ou la présentation de sujets d'intérêt personnel (loisirs, sport, culture, diffusion d'idées, etc.).

Le blog n'est pas un espace de non-droit, bien que le blogueur soit libre de pouvoir y formuler ce qu'il souhaite. Il doit respecter certaines règles ainsi que les droits des personnes qui peuvent être concernées par ses propos. Ainsi tout blogueur doit se demander avant la création de son blog ce qu'il peut faire ou ne pas faire.

Les parents sont responsables des publications de leur enfant

Les parents sont responsables des publications de leurs enfants. Ils sont censés leur donner leur autorisation pour l'ouverture de leur blog. Si au niveau pénal, les parents ne peuvent pas, sauf exception, être sanctionnés pour une infraction commise par leur enfant, ils sont tous les deux responsables civilement des actions de leur enfant s'il vit avec eux (article 1384 du code civil). En pratique cela signifie qu'ils peuvent être condamnées si leur enfant a par exemple, injurié un professeur ou utilisé une image sans autorisation.

Peut-on utiliser des photographies de ses amis ou de son professeur ?

Aux termes de l'article 9 du code civil relatif au respect de la vie privée, la diffusion et l'utilisation de photographies requièrent au préalable d'obtenir l'autorisation écrite de la personne concernée ou celle de ses parents si elle est mineure.

Le blog et la diffamation

La tenue sur un blog de propos diffamatoires, calomnieux, injurieux ou racistes à l'égard d'une personne, par exemple un enseignant ou un élève peut faire l'objet de poursuites judiciaires. Le mineur capable de discernement peut être pénalement sanctionné. Des sanctions disciplinaires peuvent également être prises par l'établissement scolaire du lycéen auteur de propos diffamatoires ou injurieux à l'égard d'un professeur ou d'un camarade de classe.

Attention, on est également responsable des commentaires des autres sur son propre blog.

Fiche n°19 : Protéger sa vie privée sur internet

Quel est le problème ?

Il faut avoir conscience que sur internet, nos activités et nos déplacements laissent des traces. Toute action que nous effectuons sur internet produit des contenus qui sont copiés afin que chaque internaute puisse en prendre connaissance. De ce fait, il est en pratique impossible d'effacer complètement une information mise sur internet : il en reste toujours une trace.

Lorsque l'on consulte une page internet, celle-ci est enregistrée dans notre ordinateur pour permettre sa visualisation : il reste ainsi une trace de notre navigation sur notre ordinateur.

De même, lorsque nous "postons" des commentaires sur le mur Facebook d'un ami, ceux-ci sont conservés dans les ordinateurs du réseau social et constituent autant de traces.

Enfin, lors de chacune de nos recherches sur internet, les moteurs collectent généralement de nombreuses informations sur nous : l'adresse IP de notre ordinateur, les informations contenues dans les cookies, les mots clés que nous avons saisis et le lien sur lequel nous avons cliqué. Au fur et à mesure de nos recherches, le moteur en vient à connaître précisément nos centres d'intérêts ainsi que toutes les publicités auxquelles nous sommes sensibles.

Les applications du Web 2.0, et notamment les réseaux sociaux, font exploser le nombre d'informations personnelles accessibles sans limitation de durée sur internet. Les photos de soirées arrosées ou de vacances en maillot de bain sont mises en ligne sur Facebook. Des plaisanteries plus ou moins douteuses, des opinions politiques, des préférences sexuelles, des relations privées sont affichées sur des blogs. Les films personnels sont diffusés sur des sites vidéo – de plus en plus souvent à l'insu des personnes concernées.

La diffusion de ces informations sur le réseau peut avoir des conséquences désastreuses : nombre de professionnels (ressources humaines, compagnies d'assurances, recherche de personnes disparues…) utilisent désormais de manière routinière des données extraites d'internet pour vérifier, compléter ou valider des dossiers de candidats, de salariés ou de clients.

Enfin, les enfants constituent trop souvent une cible idéale pour obtenir de manière déloyale des informations sur eux et leurs proches. En effet, la rapidité des échanges, l'interactivité, voire l'aspect ludique du réseau internet font des enfants des cibles idéales pour se procurer des informations toujours plus nombreuses et plus précises. Se constituent ainsi, à l'insu des parents et sans que les enfants en aient eux-mêmes conscience, des bases de données très performantes sur l'environnement social et économique des familles, qui sont susceptibles de porter atteinte à leur vie privée.

Que dit la loi ?

Les données personnelles sont les informations qui concernent une personne identifiable, par exemple, un nom, une photo, un numéro de téléphone portable, l'adresse IP attribuée par votre fournisseur d'accès…

Si des informations nous concernant figurent dans un fichier, nous avons le droit d'en demander la communication (copie lisible), la correction, voire la suppression.

La loi « *informatique et libertés* » prévoit que les données à caractère personnel doivent être conservées le moins longtemps possible. La fixation de la durée de conservation et l'existence de procédés de mise à jour doivent permettre le respect du principe du « *droit à l'oubli* ».

Qu'est ce que le droit à l'oubli ?

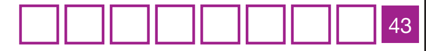
Si le cerveau humain a une capacité à oublier les informations qu'il reçoit, ce n'est pas le cas de l'ordinateur. Concrètement, le droit à l'oubli dans le monde de l'internet devrait obliger les réseaux à oublier ce que l'on a pu faire dans le passé.

On peut parler d'un droit à l'oubli numérique ou encore du droit d'effacer ses traces sur internet. Ce droit à l'oubli, c'est le droit de changer, d'évoluer, de se contredire.

Avant toute chose, il faut être conscient que la meilleure façon de se protéger est de faire attention à ce que l'on publie. Cela est difficile en pratique puisque l'utilisation des réseaux sociaux conduit à dévoiler toujours plus d'informations sur soi, sans pour autant savoir qui y aura accès, dans quel but et pour combien de temps. Ces informations peuvent être exploitées de plus en plus vite, en plus grand nombre et sont potentiellement accessibles en tout point du globe. Nous n'avons aucune garantie quant à la maîtrise des informations que nous mettons en ligne. Il est donc indispensable d'être particulièrement prudent quand on publie des informations sur internet. En effet, même si l'on souhaite partager son intimité avec des personnes choisies, le risque est de voir circuler très rapidement sur internet ou sur les téléphones mobiles des informations que l'on aurait souhaité limiter à la seule sphère privée.

Sur internet, les traces restent très longtemps et ce stockage illimité des données peut faire l'effet d'une véritable « *bombe à retardement* », notamment dans le domaine du recrutement.

Par exemple, les informations laissées sur internet peuvent être reprises des années plus tard lors, par exemple, de son inscription à la faculté, lors d'un entretien d'embauche et faire ainsi apparaître des informations très privées (informations relatives aux opinions politiques, aux orientations ou pratiques sexuelles, à la religion ou à la santé) ou peu flatteuses (une photo lors d'une soirée étudiante très arrosée) qui peuvent avoir des conséquences sur sa vie (candidature d'embauche refusée).



Les 10 conseils de la CNIL pour protéger sa vie privée sur internet
« Avant de publier, je réfléchis ! »
1// Se poser les mêmes questions que celles que vous vous poseriez dans la *« vraie vie »* lors de la diffusion de données personnelles sur internet. Exemple : est-ce que je souhaite que mes parents ou encore que tout mon lycée aient accès aux photos prises avec ma petite amie ?
2// Prendre conscience que la maîtrise des informations publiées sur internet dépend avant tout de soi. Donc, que la meilleure façon de se protéger, c'est de faire attention à ce que l'on publie.
3// Faire preuve d'une grande vigilance lors de votre inscription sur un réseau social : donner le moins d'informations possibles ou ne dire que le strict nécessaire. Evitez de dévoiler systématiquement des données personnelles à chaque inscription sur internet (Exemple : ne pas communiquer son numéro de téléphone ou l'adresse de son domicile), ne donnez pas de détails privés tels que des opinions politiques, religieuses ou des renseignements médicaux sur soi ou sur son entourage (famille ou amis).
4// Sécuriser son compte sur les réseaux sociaux en apprenant à paramétrer son profil. Dès l'ouverture d'un compte sur un réseau social, ayez le réflexe de définir votre espace de confidentialité ou si vous avez déjà un compte, pensez à limiter le nombre de personnes habilitées à consulter les éléments (textes, photos, vidéo) que vous y avez postés. Ce paramétrage permet de limiter dans une certaine mesure la diffusion de données personnelles à des catégories de personnes identifiées (ex. tous vos amis, certains amis). Ainsi, par exemple, le paramétrage de votre profil permet d'éviter l'indexation de la totalité de vos données par les moteurs de recherche. Par le biais des fonctionnalités de paramétrage de votre compte, vous pouvez ainsi à tout moment contrôler le contenu des informations qui vous concernent, rectifier voire même supprimer ces informations.
5// Modérer ses propos lorsque vous intervenez sur les blogs, forums, les *« murs Facebook »*, les *« tweets ».*
6// Eviter de publier des photos qui pourraient se révéler gênantes. Exemple : vous avez choisi de partager une de vos photos avec un de vos amis. Que se passera-t-il si demain cette personne n'est plus votre ami et s'amuse à diffuser cette photo à tout le lycée ? (un ami d'aujourd'hui n'est pas forcément un ami de demain).



7// Ne pas publier sur Internet des contenus sur autrui qui pourraient lui nuire : toujours vous demander comment vous réagiriez si on faisait la même chose pour vous ; ne vous amusez pas à créer un compte sur un réseau social à la place d'une autre personne, ne tagguez pas des photos d'amis sans les prévenir, limitez la publication d'album photos ou de vidéos et soyez vigilant sur le marquage de photos.
8// Vérifier régulièrement ce qui est publié vous concernant sur le web. Par exemple, en renseignant votre nom dans un moteur de recherche, vous pouvez découvrir à cette occasion que des informations vous concernant sont diffusées sur internet. Vous pouvez demander au responsable du site web diffusant ces informations de supprimer les pages qui vous concernent. C'est aussi à lui de faire le nécessaire auprès des moteurs de recherche pour que ces pages ne soient pas indexées.
9// Utiliser si possible un pseudonyme que vous communiquez à vos proches.
10// Ne pas communiquer ses mots de passe et ne pas choisir des mots de passe trop simples (Exemple : pas votre date de naissance ou le prénom d'un proche). Privilégiez des mots de passe différents pour chaque site sur lequel vous vous inscrivez. Pensez à verrouiller votre ordinateur et à vous déconnecter de votre compte quand vous quittez votre ordinateur (sinon n'importe qui pourrait poster des contenus à votre place.)
En collaboration avec Internet Sans Crainte

pour aller plus loin : **www. jeunes.cnil.fr**

Annexe n°1 « Mode d'emploi : comment déclarer ? »

La déclaration est une obligation légale dont le non-respect est pénalement sanctionné [14]. Tout fichier ou traitement informatisé comportant des données personnelles doit donc être déclaré à la CNIL préalablement à sa mise en œuvre, sauf s'il est expressément exonéré de déclaration. Cette procédure de déclaration peut prendre plusieurs formes selon le fichier concerné [15].

Dans tous les cas, la désignation d'un Correspondant Informatique et Libertés dispense l'organisme concerné de l'accomplissement des formalités relatives aux fichiers relevant de la déclaration simplifiée et de la déclaration normale.

1. Les dispenses de déclaration

Un certain nombre de traitements, décrits dans le tableau récapitulatif figurant ci-après, sont dispensés de déclaration par une décision de la CNIL (ex. : site web institutionnel, sites web personnels).

Par ailleurs, les fichiers de gestion des élèves et des personnels des établissements de l'enseignement secondaire n'ont pas, en principe, à être déclarés auprès de la CNIL dans la mesure où ils ont fait l'objet d'une déclaration par le Ministère de l'Education nationale (ex. : application SCOLARITE pour la gestion du fichier des élèves de collèges et des lycées).

2. La déclaration normale

Le régime de droit commun est la déclaration normale, lorsque le fichier ne relève pas d'une procédure particulière (art. 22 de la loi *« Informatique et Libertés »*) (exemples : mise en œuvre d'un système de vidéosurveillance, d'un annuaire des anciens élèves, diffusion des résultats sur internet…).

Le traitement peut être mis en œuvre dès réception du récépissé délivré par la CNIL.

Le récépissé atteste de l'accomplissement des formalités de déclaration, mais n'exonère pas le responsable du traitement des autres obligations prévues par la loi (respect de la finalité du fichier, sécurité et confidentialité, respect des droits des personnes…).

3. La déclaration simplifiée

Certains des fichiers des établissements de l'enseignement secondaire peuvent faire l'objet de déclarations simplifiées (ex : traitement ayant pour finalité la gestion des personnels des établissements privés liés ou non à l'Etat, traitement ayant pour finalité la gestion des contrôles d'accès aux locaux en référence à la norme simplifiée n°46, des horaires et de la restauration en référence à la norme simplifiée n°42).

(14) Article 226-16 du code pénal : « Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

(15) Le régime déclaratif des principaux fichiers mis en œuvre par les établissements de l'enseignement supérieur est indiqué dans le tableau récapitulatif figurant ci-après.

4. Les formalités particulières

Certains traitements des établissements d'enseignement secondaire peuvent relever d'un régime d'autorisation ou de demande d'avis. Il s'agit de régimes plus protecteurs, qui s'appliquent aux fichiers considérés comme *« sensibles »* ou comportant des risques pour la vie privée ou les libertés.

*** La procédure d'autorisation concerne (art. 25) :**

- les traitements qui comportent des données dites sensibles (16);
- les traitements qui comportent des données relatives aux infractions ou condamnations ;
- les traitements qui procèdent à l'interconnexion de fichiers dont les finalités correspondent à des intérêts publics différents ;
- les traitements de données comportant des appréciations sur les difficultés sociales des personnes.
- les traitements qui utilisent des données biométriques (**Exemple :** le contrôle de l'accès au restaurant scolaire reposant sur l'utilisation d'un dispositif biométrique)

Le traitement devra respecter en tous points le cadre fixé par l'autorisation délivrée par la CNIL.

*** La procédure de demande d'avis (art. 27)** concerne principalement les traitements comportant le numéro de sécurité sociale (NIR) ou nécessitant une interrogation du répertoire national d'identification des personnes physiques (RNIPP), et les téléservices de l'administration électronique comportant un identifiant (Exemple : formulation par internet des vœux d'affectation dans l'enseignement supérieur pour les élèves de classe de terminale comme l'application RAVEL pour l'Ile-de-France).

La demande d'avis doit être accompagnée d'un projet d'arrêté ou de décision de l'organe délibérant, destiné à autoriser le traitement une fois l'avis de la CNIL rendu.

5. Une fois le dossier complété :

- dans le cas d'une télédéclaration, la CNIL adresse immédiatement après envoi un accusé de réception électronique (17);

La plupart des formalités préalables peuvent être effectuées à partir du site web de la CNIL (www.cnil.fr).

(16) Les données dites « sensibles » sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou la vie sexuelle des personnes (article 8 de la loi « Informatique et Libertés »).

(17) Ne pas confondre l'accusé de réception d'un dossier adressé à la CNIL avec le courrier de la CNIL qui constitue le seul feu vert pour la mise en œuvre d'un fichier ou d'un traitement de données personnelles. En fonction de la procédure effectuée, ce courrier prendra la forme d'un récépissé (déclaration), d'une autorisation (demande d'autorisation) ou d'un avis (demande d'avis).



Annexe n°2 : Tableau récapitulatif : Dois-je déclarer mon fichier à la CNIL ? Comment ?

Rappel : les traitements n'ont pas à faire l'objet de déclaration (18) lorsqu'un Correspondant Informatique et Libertés a été désigné.

POUR LE SECOND DEGRE (COLLEGES ET LYCEES)	
DECLARATIONS A EFFECTUER	**FINALITES DES TRAITEMENTS**
PAS DE DECLARATION	- Gestion du fichier des élèves des collèges et des lycées du secteur public et privé sous contrat (application SCOLARITE). ***(déclaration du Ministère de l'Education nationale - arrêté du 22 septembre 1995)*** - Gestion des infirmeries (application S.A.G.E.S.S.E). ***(déclaration du Ministère de l'Education nationale - arrêté du 4 mai 2001)*** - Gestion des bourses nationales de l'enseignement du second degré par les inspections académiques (application B.A.L.I). ***(normalement déclaré par chaque inspection académique - arrêté du 11 mars 1994 modifié le 28 septembre 1999)*** - Gestion des concours et des examens scolaires par les rectorats et les inspections académiques (application S.A.G.A.C.E.S). ***(normalement déclaré par chaque rectorats et inspections académiques - arrêté du 12 juillet 1995 pris par le Ministère de l'Education nationale)*** - Gestion des personnels des établissements publics locaux (application nationale, Emplois, Postes, Personnels - E.P.P). ***(déclaration du Ministère de l'Education nationale - arrêté du 2 juillet 1992)*** - Bouquet de services internet personnalisés proposés aux personnels au niveau académique (outil *« I-PROF »*). ***(déclaration du Ministère de l'Education nationale - arrêté du 17 octobre 2003)*** - Les sites web vitrines ou institutionnels permettant par exemple l'envoi de lettre d'information. ***(à condition de respecter la dispense n° 7)*** - Les sites web personnels : sites diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'activités exclusivement personnelles tels que les *« blogs »*. ***(à condition de respecter la dispense n° 6)***

(18) Par contre les demandes d'autorisation ou d'avis à la CNIL subsistent.

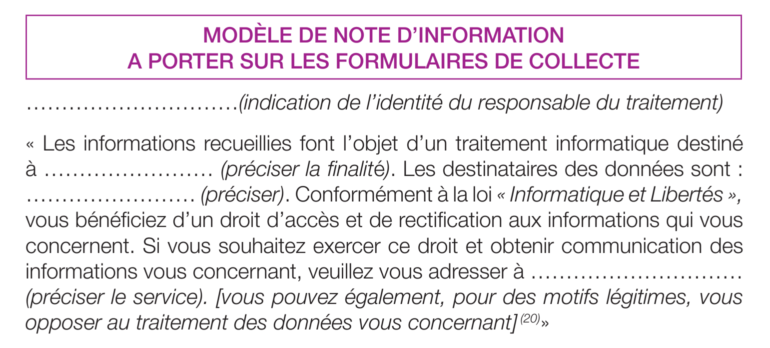
DECLARATIONS SIMPLIFIEES	- Gestion des personnels des établissements d'enseignement privés (lié ou non à l'Etat par contrat). ***(en référence à la norme simplifiée n° 46)*** - Gestion des contrôles d'accès aux locaux, des horaires et de la restauration. ***(en référence à la norme simplifiée n° 42[19].)***
DEMANDE D'AUTORISATION	Contrôle de l'accès au restaurant scolaire reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main (biométrie). ***Engagement de conformité à l'autorisation unique n° 009 adoptée par la CNIL par une délibération n° 2006-103 du 27 avril 2006***
DEMANDE D'AVIS (Téléservice de l'administration électronique)	- Inscription par internet à des examens, à des concours et dans des établissements d'enseignement (création d'un compte utilisateur). - Formulation par internet des vœux d'affectation dans l'enseignement supérieur pour les élèves de classe de terminale (exemple : application RAVEL pour l'Ile-de-France). - Les sites web portail dans le cadre des espaces numériques de travail (ENT). Engagement de conformité à l'arrêté « *ENT* » du 30 novembre 2006 pris par le Ministère de l'éducation nationale (acte réglementaire unique n° 003)
AUTRE Le principe est celui d'une déclaration normale mais il existe des exceptions. Pour les connaître, consulter le site de la CNIL.	Tout autre traitement automatisé, dès lors qu'il n'est pas conforme aux normes élaborées par la CNIL, notamment : - vidéosurveillance - annuaire des anciens élèves - diffusion de résultats sur Internet…

(19) Cette norme ne concerne pas les traitements recourant à un procédé de reconnaissance biométrique, qui sont soumis à autorisation.



Annexe n°3 Modèles de clauses ou de mentions d’information

Modèles de note d’information



MODÈLE DE NOTE D’INFORMATION
A PORTER SUR LES FORMULAIRES DE COLLECTE

..............................*(indication de l’identité du responsable du traitement)*

« Les informations recueillies font l’objet d’un traitement informatique destiné à .... *(préciser la finalité)*. Les destinataires des données sont : .... *(préciser)*. Conformément à la loi « *Informatique et Libertés* », vous bénéficiez d’un droit d’accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à .... *(préciser le service). [vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant]* [(20)] »

MODÈLE DE NOTE D’INFORMATION
À UTILISER SUR LE DOSSIER D’INSCRIPTION DES ÉLÈVES

« Les informations recueillies par *[préciser ici l’identité du responsable du traitement – en l’espèce l’établissement XX]* font l’objet d’un traitement informatique destiné à assurer la gestion administrative et pédagogique des élèves, à établir des statistiques par le Ministère de l’éducation nationale. Les maires des communes de résidence des élèves, les conseillers d’information et d’orientation, les agents habilités des collectivités locales organismes de sécurité sociale, les caisses d’allocations familiales sont également destinataires d’informations nécessaires à l’accomplissement de leurs missions. Conformément à la loi « *Informatique et Libertés* », vous bénéficiez d’un droit d’accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à .... *[Préciser le service chargé du droit d’accès - en principe, ce droit doit pouvoir s’exercer auprès du responsable d’établissement dans lequel l’étudiant est inscrit].* »

(20) A ne pas faire figurer si le traitement présente un caractère obligatoire.

MODÈLE DE NOTE D'INFORMATION SUSCEPTIBLE D'ÊTRE AFFICHÉE

«Le(s) service(s) .... (citer le nom du ou des services concernés) dispose(nt) de moyens informatiques destinés à gérer plus facilement.................................... (indiquer la finalité du traitement).

Les informations enregistrées sont réservées à l'usage du (ou des) service(s) concerné(s) et ne peuvent être communiquées qu'aux destinataires suivants : .... (préciser les destinataires).

Conformément aux articles 39 et suivants de la loi « *Informatique et Libertés* », toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au service .... (citer le nom du service ou des services concernés). [toute personne peut également, pour des motifs légitimes, s'opposer au traitement des données la concernant](21)»

MODÈLE DE CLAUSE DE CONFIDENTIALITÉ DANS LE CADRE D'UN MARCHÉ OU D'UN CONTRAT DE SOUS-TRAITANCE

Les supports informatiques fournis par l'établissement et tous documents, de quelque nature qu'ils soient, résultant de leur traitement par la société ...., restent la propriété de l'établissement.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226.13 du code pénal). Conformément à l'article 34 de la loi n°78-17 du 6 janvier 1978 modifée relative à l'informatique, aux fichiers et aux libertés, la société .... s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

La société .... s'engage donc à respecter, de façon absolue, les obligations suivantes et à les faire respecter par son personnel, c'est-à-dire à :

- ne prendre aucune copie des documents et supports d'informations confiés par la société .... et utilisés par la société .... à l'exception de ceux nécessaires pour les besoins de l'exécution de sa prestation, objet du présent contrat ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;

(21) A ne pas faire figurer si le traitement présente un caractère obligatoire.



- prendre toutes les mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- prendre toutes les mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de la durée du présent contrat ;

et en fin de contrat à :

- procéder à la destruction de tous les fichiers manuels ou informatisés stockant les informations saisies ;

ou à :

- restituer intégralement les supports d'informations selon les modalités prévues au présent contrat.

A ce titre, également, la société .... ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché. Les supports d'informations qui lui seront remis devront être traités sur le territoire français métropolitain.

L'établissement se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par la société ....

Il est rappelé que, en cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-17 et 226-5 du code pénal.

L'établissement pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

Annexe n°4 Lexique

LEXIQUE INFORMATIQUE ET LIBERTES	
CNIL	Autorité administrative indépendante, composée d'un collège pluraliste de 17 commissaires, provenant d'horizons divers (4 parlementaires, 2 membres du Conseil économique et social, 6 représentants des hautes juridictions, 5 personnalités qualifiées désignées par le président de l'Assemblée nationale (1), par le président du Sénat (1), par le conseil des ministres (3). Le mandat de ses membres est de 5 ans. Le président est élu par ses pairs.
Correspondant Informatique et Libertés	Créé en 2004, le correspondant informatique et libertés (CIL) est chargé d'assurer de manière indépendante le respect des obligations prévues par la loi « *Informatique et Libertés* » ; en contrepartie de sa désignation, les traitements de données personnelles les plus courants sont exonérés de déclaration auprès de la CNIL.
Destinataire	Personne habilitée à obtenir communication de données enregistrées dans un fichier ou un traitement en raison de ses fonctions.
Donnée biométrique	Caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales…).
Donnée personnelle	Toute information identifiant directement ou indirectement une personne physique (ex. nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale.....).
Donnée sensible	Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle d'une personne. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.
Droit à la protection des données personnelles	Le droit à la protection des données à caractère personnel est inscrit dans la charte des droits fondamentaux de l'Union européenne au titre des libertés fondamentales telles que la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information ou le respect de la vie privée et familiale, etc.
Droit à l'information	Toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union Européenne.

Droit d'accès direct	Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.
Droit d'accès indirect	Toute personne peut demander que la CNIL vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique.
Droit d'opposition	Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection, notamment, commerciale.
Droit de rectification	Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.
Finalité d'un traitement	Objectif principal d'une application informatique de données personnelles. Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.
Formalités préalables	Ensemble des formalités déclaratives à effectuer auprès de la CNIL avant la mise en œuvre d'un traitement de données personnelles ; selon les cas, il peut s'agir d'une déclaration ou d'une demande d'autorisation.
Formation restreinte	Pour prendre des mesures à l'encontre des responsables de traitement qui ne respectent pas la loi informatique et libertés, la CNIL siège dans une formation spécifique, composée de six membres appelée «*formation restreinte*». À l'issue d'une procédure contradictoire, cette formation peut notamment décider de prononcer des sanctions pécuniaires pouvant atteindre 300 000 €.
Listes d'opposition	Les listes d'opposition recensent les personnes qui ont fait connaître leur opposition à être prospectées dans le cadre d'opérations de marketing.
NIR	Le Numéro d'Inscription au Répertoire ou numéro de sécurité sociale est attribué à chaque personne à sa naissance sur la base d'éléments d'état civil transmis par les mairies à l'INSEE.
Responsable du traitement	Personne qui décide de la création d'un fichier ou d'un traitement de données personnelles, qui détermine à quoi il va servir et selon quelles modalités il sera mis en œuvre.

Séance plénière	C'est la formation qui réunit les 17 membres de la CNIL pour se prononcer sur des traitements ou des fichiers et examiner des projets de loi ou de décrets soumis pour avis par le Gouvernement.
Traitement de données	Collecte, enregistrement, utilisation, transmission ou communication d'informations personnelles, ainsi que toute exploitation de fichiers ou bases de données, notamment des interconnexions.
Transfert de données	Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.



Document Imprimé sur papier 100% recyclé

Une difficulté ? Une hésitation ?

Plus d'informations sur **www.cnil.fr,**

Une permanence de renseignements juridiques
par téléphone est assurée tous les jours
de 10h à 12h et de 14h à 16h
au **01 53 73 22 22**

Vous pouvez en outre adresser toute demande
par télécopie au **01 53 73 22 00**



www.cnil.fr

8 rue Vivienne - CS 30223
75083 Paris cedex 02
Tél : 01 53 73 22 22
Fax : 01 53 73 22 00